

Ad Hoc Committee
Adams County Personnel & General Administrative Policies
March 10, 2009 – 4:00 p. m. - Room A260

Meeting called to order by Chair Stuchlak with all members in attendance. Also attending were Corporation Counsel and Administrative Coordinator/Director of Finance.

The meeting was properly noticed.

Motion by Ward/West to approve the agenda. MC by UVV.

Motion by Ward/Sumpter to approve the minutes of the last meeting. MC by UVV.

The Chair requested that in the future the agenda item "Feed back from Department Heads" be added right after approval of minutes.

All numbering in this Chapter 9 will be in the same format as the rest of the Adams County Personnel & General Administrative Policies.

Management Information System (page 3 #2)

MIS houses, administers and operates all servers, infrastructure and security equipment for Adams County agencies, unless special exceptions are granted by **the MIS Department with consultation with Corporation Counsel if need be, [LB1]** the MIS Department is the custodian of the County's information resources and implements the policies set forth in this document. MIS acts on behalf of Adams County Government and Department/Division Heads to secure information, applications, systems and networks, to provide authorized access to approved personnel and to monitor, detect, investigate and report on actual or suspected security breaches or incidents. **[LB2]**

Physical Security (Section 3 (1)) page 3

It shall be the policy of Adams County that all data centers and closets are secured, restricted areas. Access shall be granted to only those individuals who have a mission essential business need and who have been appropriately cleared. County data centers contain data, which is sensitive, personal in nature and in some cases protected by law. Data centers are not common workspaces. Traffic in the data centers shall be kept to a minimum. Unaccompanied access to data centers and closets shall require HIPPA Training and the signing of the County ~~Privacy~~ **Non Disclosure** Agreement.

Comment [DMS1]: Privacy agreement is attached to end of policy, it was being edited by Corp. Counsel at the time.

Data Security (Section 3 (3) (f)) page 4

All Computers are required to have an idle PC lockout after 15 minutes of idle time. **All users are encouraged to log off or lock (Ctrl+Alt+Del) the computer system before leaving their computer unattended.** MIS will reserve the right to log off the computer after 1 hour of inactivity for network security purposes and to allow maintenance to be performed on the computers during off hours. **[LB4]**

Password Security (Section 3 (4) (f) see Section 3 (3)(f)) page 4

~~Computers will lock automatically after 15 minutes of inactivity. **[LB5]** All users are encouraged to log off or lock (Ctrl+Alt+Del) the computer system before leaving their computer unattended.~~

File Security (Section 3 (5)(c)) page 5

Removable disk storage media – Each employee is responsible for the maintenance and security of the data they store onto removable storage media. ~~No PHI (Personal Health Information) data should reside on removable storage media~~ **must be consistent with the Adams County HIPPA Policy.** Users must ensure the devices are password protected if they contain county data. Users must also password protect any confidential data should these devices be lost and fall into a person's hands who is not authorized to see the information.

Workstation Security

Monitors should generally be kept from the plain view of anyone who does not have the appropriate access or clearance to information that may be displayed. Site surveys should be conducted **semi-annually by the MIS Department and a report of any infraction shall be reported to the respective Department Head.** ~~by each department to check for unauthorized viewing from the following sources, and is especially critical where compliance related information may be displayed:~~

- ~~(i) Outside windows~~
- ~~(ii) Public hallways~~
- ~~(iii) Public reception areas~~
- ~~(iv) Reflection off of other objects~~

John West was excused at 6:00 p.m.

Incident response and reporting (Section 3 (7) Page 6

~~It is the intention of Adams County to~~ **will** adhere to a standardized procedure of responding to security incidents, investigating these events, documenting the results of those investigations and taking appropriate action to meet operational and legal requirements for addressing the incident. The county shall maintain preventative measures to avoid any reasonably anticipated events that would compromise the confidentiality, integrity or availability of data stored on the County network or County owned devices. It is also the intent of this policy that each investigation contains recommendations and courses of action that will lessen the likelihood of a recurrence whenever possible. This applies to all actual or suspected security incidents on Adams County networks, including attacks emanating from outside the County, business partner connections, wireless and remote access, or the theft or unauthorized removal of media, data, storage devices, disks or CDs. This policy applies to all county employees, elected officials, boards, committee and commission members who have access to County systems, interns, contractors, affiliated or tenant agencies, business partners and volunteers.

Section (7)(a)(iv) (v) page 7

IV Inappropriate usage: ~~An individual who~~ **The** accesses **of** systems, networks or data without full compliance ~~with~~ **of** all policies. ~~violates the County Acceptable Use Standards.~~

(v) Mixed or blended attack: ~~It is possible that~~ **An** incident would be comprised of multiple categories or incidents. The relative severity of a blended attack would be ~~determined~~ based on the information gathered at the time of the attack or detection.

Section (7)(b)(i) page 7

Preparation and prevention: the process of creating a policy, severity index and reporting structure for incidents, and creating a security posture which may prevent incidents from occurring **or reoccurring**.

The committee will start with Section 7 (c) Incident response and reporting procedures.

Ward asked to be excused from the next meeting.

Next meeting will be March 24th at 4:00 p.m. in Room A260.

Motion by Sumpter/Stuchlak to adjourn. MC by UVV. Meeting adjourned at 6:26 p.m.

Respectfully submitted,

Bev Ward, Acting Recording Secretary